REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

In the specification, paragraph numbers [0008], [0048] and [0054] have been amended.

Claim 14 and the first of duplicate claims 29 and 46 are requested to be cancelled.

Claims 1-5, 15, 19-27, 45-49 and 52-55 are currently being amended.

This amendment adds, changes and/or deletes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 1-12, 15-40 and 42-68 are now pending in this application.

In the Final Action dated October 31, 2005, the Examiner objected to the specification due to a number of informalities identified in paragraph numbers [0008], [0048] and [0054]. In response to these objections, Applicant has corrected each of the formalities identified by the Examiner. Applicant has also made a number of other formal corrections to these paragraphs. In making these amendments, Applicant has submitted no new matter into the specification. Regarding any other issues concerning the specification, the Examiner is asked to specifically identify these issues.

The Examiner objected to claim 24 on the grounds that the term "of" appeared to be missing from line 17 and/or 18 of the claim. Applicant has therefore added this term in accordance with the Examiner's comments. The Examiner also noted that Applicant's previous amendment and reply included two claim nos. 29 and 46. In order to address this deficiency, Applicant has deleted the first claim 29 and the first claim 46. In making these deletions, Applicant fully intends to maintain the "second" claims 29 and 46 in the

application. In addition, Applicant notes that the duplicate claims were the result of an administrative error, and Applicant therefore does not intend to surrender any claim scope, both generally and in relation to the Doctrine of Equivalents, by canceling these claims.

The Examiner rejected claim 14 under 35 U.S.C. §112, second paragraph as being indefinite due to, in the Examiner's view, the limitation "without a smart card" not being sufficiently described in the specification. Solely to advance the prosecution of the present application, Applicant has canceled claim 14. However, Applicant wishes to emphasize that, in canceling this claim, Applicant is not agreeing with any insinuation that non-smart card separate units are not covered by claim 5 or any other claims that only discuss a "separate unit." The specification and claims repeatedly refer to the use of a separate unit in conjunction with the present invention, and smart cards of various types are only described in terms of particular embodiments of the present invention. In this light, Applicant is taking no other position than that the term "separate unit" is to be given its ordinary meaning, and this meaning includes, but is not limited to, smart cards. In the event that the Examiner disagrees with this position, then he is strongly encouraged to contact the attorneys for Applicant to discuss this issue in greater detail.

The Examiner has rejected claims 1, 3-12, 14-19, 21-24, 27-40, 42-44 and 46-68 under 35 U.S.C. §103(a) as being unpatentable over PCT Publication No. WO97/24831, in the name of Ichikawa, in view of European Publication No. 0538216, in the name of Anvret et al. For each of the independent claims, the Examiner has asserted that the Ichikawa references teach all of the features of the claims except for the use of public and private keys, but that this feature could be found in the Anvret et al. reference and that it would have been obvious to combine the two references. The Examiner also rejected claims 2, 20, 25, 26 and 45 under 35 U.S.C. §103(a) as being unpatentable over the Ichikawa and Anvret et al. references and in further view of U.S. Patent No. 5,845,519, issued to Weiss.

Applicant respectfully traverses each of these rejections. In particular, and for the reasons below, Applicant respectfully submits that the prior art references cited by the Examiner do not teach or suggest a master secret code of the type described in the amended claims.

As has been discussed previously, the currently-pending claims describe a master secret key or code which is generated or calculated by a wireless communication device to calculate a signature, which is then transmitted to a data communication apparatus. The generation or calculation of the master secret key or code occurs in response to the wireless communication device receiving a message from the data communication apparatus, with this message including information such as the data communication apparatus's public key.

The master secret key or code can then be determined by the data communication apparatus based upon information it already has in its possession. The calculated master secret key or code is then saved on the memory or memory means for later use. As has been discussed at length, this saving of the calculated code provides the benefit of the wireless communication device not having to regenerate or recalculate a master secret key or code at a later time, saving valuable computational resources.

In the previous Official Actions, the Examiner has taken the position that the Ichikawa reference discusses the generation of a master secret code, and that this code is stored. The Examiner has relied upon page 4, lines 10-12 and page 6, lines 16-18 to support this position. However, this position fails to address related language in each of the independent claims. In particular, independent claim 1 (before the present amendments) specifically noted that the master secret code is generated upon reception of the message from the data communication apparatus including information such as the data communication apparatus's public key. In other words, the master secret code is not first generated until it has received other information from the data communication apparatus that is necessary for signature calculation.

This specific feature is not taught or even hinted at in the Ichikawa reference. In the Ichikawa reference, the master key is stored in a secured area of permanent memory (pg. 6, ll. 15-16), and the same master key is also stored on the server side (pg. 7, ll. 11-14). At the beginning of an attempted transaction between the client and server, both devices already have the master key in their possession (as well as all of the potential series numbers), and this information is used to generate a derived key each time that authentication is attempted (pg. 10, l. 14-pg. 12, l. 2; FIG. 2). Furthermore, and as has been discussed in earlier

communications, the authentication process involves sets of parallel computations by both the client and the server. Importantly, however, at no time during the authentication process does the client device ever have to generate the master key, much less have to generate a master key in response to any message received from the server.

The present invention as described in claim 1, on the other hand, specifically describes the generation as a situation where the master secret code is not generated or calculated until a message is received from the data communication apparatus. This provides at least one important advantage over the system described in Ichikawa. In the Ichikawa system, both the server and the client already have in their possession the relevant variables (particularly the master key and the potential series numbers), that may be used during the derivation process. In independent claim 1, on the other hand, the data communication apparatus does not have an important variable in its possession—the master secret code—before a first connection process begins. Because, before an initiation secure connection process, the master secret code has not even been created, this situation creates additional security by ensuring that both devices cannot have the master secret code before a first authentication process is initiated.

In addition to the above, it should also be noted that no other variable discussed in the Ichikawa reference can meet the limitation at issue. As has been discussed in previous communications, the derived key in the Ichikawa reference must be generated with each transaction, and the derived key is not stored for later use. Additionally, individual series numbers are not generated by the wireless communication device in response to a message, and there is no indication that the selected series number is saved on the memory or memory means.

For all of the above reasons, Applicant submits that the Ichikawa reference does not teach or suggest the generation of a master secret code or key in response to or upon receipt of a message from a data communication apparatus as described in claim 1.

With regard to the Anvret et al. reference, Applicant wishes to reiterate its prior arguments regarding the inapplicability of this reference with regard to the master secret code of the pending claims. In particular, the Anvret et al. reference explicitly teaches against the

saving of the master secret code (X). In fact, the specific section cited by the Examiner in the October 31, 2005 Official Action notes that "by varying X for each session, two sessions will never have the same key." Therefore, the Anvret et al. reference clearly does not teach the saving of the master secret code; in fact it teaches against it.

Although Applicant believes that independent claim 1 is patentable over the cited prior art, because there is no generation of the master secret code upon receipt of a message from the data communication apparatus, Applicant has amended the claim to more clearly identify the importance of this feature. Claim 1 has been amended so that the words "upon receipt of" have been replaced with "in response to" the message comprising the public key from the data communication apparatus. As this point is clearly noted throughout the application, and as one skilled in the art would clearly understand that an action undertaken upon receipt of the message would inherently be undertaken in response to the message , Applicant submits that no new matter is being added with this amendment.

In light of the above, similar amendments have also been made to the other independent claims in the application, particularly noting that the master secret code is generated or calculated in response to receipt of a message from the data communication apparatus. Because none of the references cited by the Examiner discuss or even suggest such a feature, Applicant submits that each of independent claims 1, 5, 15, 19, 22, 23, 24 and 46 are allowable over the Ichikawa and Anvret et al. references. Furthermore, because all of the other claims in the present application are dependent upon these independent claims, Applicant submits that each of the dependent claims are allowable over the prior art for substantially the same reasons.

With regard to the Examiner's rejection of claims 2, 20, 25, 26 and 45 under 35 U.S.C. §103(a), Applicant submits that, because these claims are all dependent upon the independent claims discussed above, each of these claims is allowable for at least the same reasons. However, Applicant wishes to separately note that the Ichikawa reference unequivocally teaches that the master key used therein should be stored "in a secured area of permanent memory" (pg. 4, ll. 5-8). In other words, Ichikawa explicitly teaches storing a master key in a location such that is permanently stored. Therefore, Applicant submits that

one skilled in the art would not be motivated to modify the Ichikawa reference to have the master key stored for only a predefined period of time, because the Ichikawa reference itself instructs a person to have the master key permanently stored. Applicant therefore submits that these claims are patentable over the prior art for this reason as well.

Lastly, Applicant notes that it has made a number of other minor amendments to the claims. For example, Applicant has changed the word "said" to "the." Applicant has also corrected potential antecedent basis issues in certain locations in the claims by changing "key" to "code" in selected locations. Applicant has also removed reference to the master secret code being stored at the data communication apparatus from claim 1, as this feature is not necessary for the patentability of the claim. In general, these amendments are being made for consistency and clarity purposes only, and none of these amendments are intended to narrow the scope of the amended claims.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 06-1450. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 06-1450. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 06-1450.

Date April 28, 2006

FOLEY & LARDNER LLP
Customer Number: 27433
Telephone: (312) 832-4553
Facsimile: (312) 832-4700

Respectfully submitted,

By _____

G. Peter Albert, Jr.
Attorney for Applicant
Registration No. 37,268